

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-090039

(43)Date of publication of application : 31.03.2000

(51)Int.Cl.

G06F 13/00
H04M 11/08
// G10K 15/04

(21)Application number : 10-260132

(71)Applicant : SONY CORP

(22)Date of filing : 14.09.1998

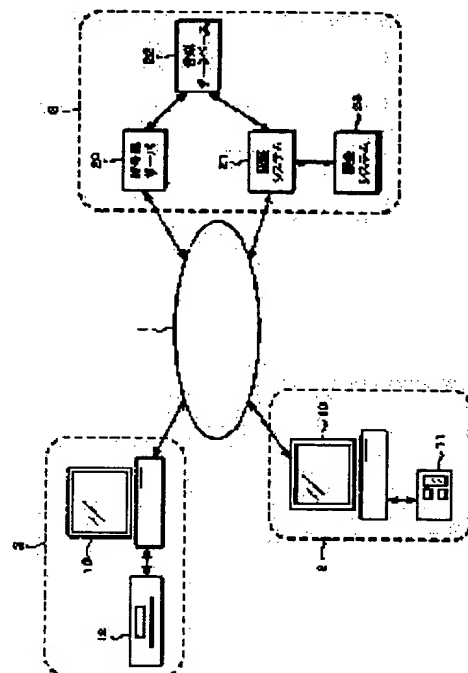
(72)Inventor : BIZEN NAOTO

(54) MUSIC DISTRIBUTING METHOD, TRANSMITTING DEVICE AND METHOD AND REPRODUCING DEVICE AND METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To sufficiently consider the protection of the copyright of distributed music data in a system distributing music data.

SOLUTION: A music server 3 and clients 2 are connected to the Internet 1. In the clients 2, a public key and a secret key are produced based on an ID proper to a reproducing device 11. The public key is sent to the server 3 to be registered and the secret key is held by the device 11. A client 2 requests the server 3 to distribute music data. Music data extracted from a music DB 22 is enciphered with the registered public key. The enciphered music data are transmitted to the client 2 and are stored in the reproducing device 11. At the time of reproducing them, the music data are reproduced while being decoded with the secret key held by the device 11. The music data stored in the device 11 can not be reproduced by other reproducing devices because they are enciphered with the key produced based on the ID proper to the device 11.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-90039

(P2000-90039A)

(43)公開日 平成12年3月31日(2000.3.31)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)	
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 Z	5 B 0 8 9
H 0 4 M 11/08		H 0 4 M 11/08		5 D 1 0 8
// G 1 0 K 15/04	3 0 2	G 1 0 K 15/04	3 0 2 D	5 K 1 0 1

審査請求 未請求 請求項の数11 O L (全 16 頁)

(21)出願番号 特願平10-260132

(22)出願日 平成10年9月14日(1998.9.14)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 尾前 尚登

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74)代理人 100082762

弁理士 杉浦 正知

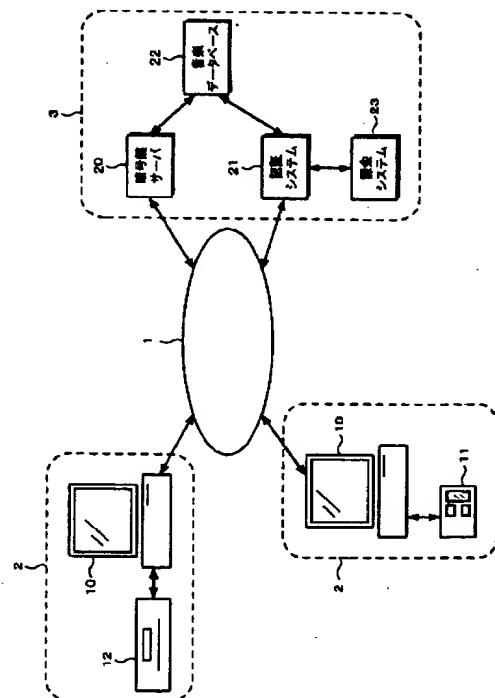
最終頁に続く

(54)【発明の名称】 音楽配信方法、送信装置および方法、ならびに、再生装置および方法

(57)【要約】

【課題】 音楽データを配信するシステムにおいて、配信された音楽データの著作権の保護を十分に配慮する。

【解決手段】 音楽サーバ3とクライアント2とがインターネット1に接続される。クライアント2において、再生装置11固有のIDに基づき公開鍵及び秘密鍵が作成される。公開鍵は、サーバ3に送られ登録され、秘密鍵は、装置11に保持される。クライアント2からサーバ3に対して、音楽データの配信が要求される。音楽DB22から取り出された音楽データに対して、登録された公開鍵で暗号化が施される。暗号化された音楽データがクライアント2に送信され、再生装置11に保存される。再生時には、装置11に保持された秘密鍵で音楽データが復号化されながら再生される。装置11に保存された音楽データは、装置11固有のIDに基づき作成された鍵で暗号化されているため、他の再生装置では再生できない。



【特許請求の範囲】

【請求項1】 端末装置から要求された音楽データを、端末装置に対して配信する音楽配信方法において、端末装置からの音楽データ配信の要求を受け付ける第1のステップと、

上記要求に基づき上記音楽データを上記端末装置に対して配信する第2のステップと、

上記要求があった上記端末装置の識別情報と、上記要求された上記音楽データとを関連付ける管理情報を蓄積する第3のステップと、

上記要求に基づき課金処理を行う第4のステップとを有し、

上記第1のステップで端末装置から音楽データ配信の要求を受け付けたときに、上記第3のステップでの上記管理情報に基づき、該端末装置による該音楽データ配信に対して上記第4のステップでの上記課金処理による課金が既に行われていると判断された場合、上記第4のステップで、課金をしないように処理するようにしたことを特徴とする音楽配信方法。

【請求項2】 端末装置から要求された音楽データを、端末装置に対して配信する送信装置において、音楽データを保存する音楽データ保存手段と、端末装置からの音楽データ配信の要求を受信する受信手段と、

上記受信手段によって受信された要求に基づき上記音楽データ保存手段から音楽データを出力する音楽データ出力手段と、

上記音楽データ出力手段によって出力された上記音楽データに対して暗号化を施す暗号化手段と、

上記暗号化された上記音楽データを上記端末に対して送信する送信手段とを有することを特徴とする送信装置。

【請求項3】 請求項2に記載の送信装置において、端末装置で秘密鍵と共に作成された公開鍵を受信する鍵受信手段と、

上記鍵受信手段で受信された上記公開鍵と、該公開鍵を作成した端末装置情報とを管理する鍵管理手段とをさらに有し、

上記暗号化手段は、上記鍵管理手段の管理情報に基づき、上記要求のあった上記端末装置に対応した上記公開鍵によって上記音楽データに対する上記暗号化を施すことを特徴とする送信装置。

【請求項4】 請求項2に記載の送信装置において、上記音楽データ保存手段では、音楽データは、圧縮符号化されて上記保存されていることを特徴とする送信装置。

【請求項5】 記憶媒体に記憶されたデジタルオーディオデータからなる音楽データを再生する再生装置において、

他の再生装置と区別するための識別情報を保持する識別情報保持手段と、

暗号化された音楽データが記憶される音楽データ記憶手段と、

再生時に、上記音楽データ記憶手段に記憶されている音楽データを読み出し、上記暗号を復号化する復号化手段と、

上記復号化手段から出力された音楽データをアナログ変換して音声信号として出力する音声信号出力手段とを有することを特徴とする再生装置。

【請求項6】 請求項5に記載の再生装置において、上記復号化手段は、上記音楽データ記憶手段に記憶されている音楽データを読み出しながら、上記復号化を行うことを特徴とする再生装置。

【請求項7】 請求項5に記載の再生装置において、上記識別情報に基づき公開鍵と共に作成された秘密鍵を保存する秘密鍵保存手段をさらに有し、

上記復号化手段は、上記鍵保存手段に保存された上記秘密鍵によって上記暗号の上記復号化を行うことを特徴とする再生装置。

【請求項8】 請求項5に記載の再生装置において、上記記憶手段は、半導体メモリからなることを特徴とする再生装置。

【請求項9】 端末装置から要求された音楽データを、端末装置に対して配信する送信方法において、音楽データを保存する音楽データ保存のステップと、端末装置からの音楽データ配信の要求を受信する受信のステップと、

上記受信のステップによって受信された要求に基づき上記音楽データ保存のステップで保存された音楽データを出力する音楽データ出力のステップと、

上記音楽データ出力のステップによって出力された上記音楽データに対して暗号化を施す暗号化のステップと、上記暗号化された上記音楽データを上記端末に対して送信する送信のステップとを有することを特徴とする送信方法。

【請求項10】 記憶媒体に記憶されたデジタルオーディオデータからなる音楽データを再生する再生方法において、

他の再生装置と区別するための識別情報を保持する識別情報保持のステップと、

暗号化された音楽データが記憶される音楽データ記憶のステップと、

再生時に、上記音楽データ記憶のステップに記憶されている音楽データを読み出し、上記暗号を復号化する復号化のステップと、

上記復号化のステップから出力された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする再生方法。

【請求項11】 端末装置からサーバに対して音楽データの配信が要求され、該要求に基づきサーバから端末装置に対して音楽データの配信を行う音楽配信方法におい

て、
端末装置からサーバに対して音楽データ配信を要求する音楽データ配信要求のステップと、

上記音楽データ配信要求のステップで要求された該音楽データが該端末装置に対して既に配信したことがあるかどうか調べられ、その結果に基づき、新規の要求であるとされれば課金を行い、過去に配信したことがあると判断されれば上記課金を行わない課金処理のステップと、

上記音楽データ配信要求のステップで要求された上記音楽データに対して、予め作成された、上記端末装置に固有の第1の鍵で暗号化を施す暗号化のステップと、
上記暗号化された上記音楽データを上記端末装置に送信する送信のステップと、

上記送信のステップで送信された上記音楽データを受信し、記憶媒体に記憶する記憶のステップと、
再生時に、上記記憶媒体から上記音楽データを読み出し、上記読み出された音楽データに施されている上記暗号を、予め作成された上記端末装置に固有の第2の鍵で、上記読み出しに伴い復号化する復号化のステップと、

上記復号化された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする音楽配信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、著作権に配慮しつつ、ユーザが無駄なく音楽配信を利用することができるような音楽配信方法、送信装置および方法、ならびに、再生装置および方法に関する。

【0002】

【従来の技術】現在、インターネットなどのネットワークや、衛星を用いたデータ通信の発達に伴い、多数の音楽データを蓄積した音楽配信サーバから、ユーザに対して音楽データの配信を行うサービスが出現しつつある。

【0003】この音楽配信システムの一例として、音楽配信サーバには、例えばデジタルオーディオデータからなる音楽データが所定の方式で圧縮符号化され、多数蓄積される。ユーザは、パーソナルコンピュータなどを用いて、例えばインターネットを介して音楽配信サーバと接続し、音楽配信サーバに蓄積されている音楽データの中から所望の音楽データを選択し、ダウンロードを要求する。音楽配信サーバは、このダウンロード要求に基づき音楽データを検索し、そのデータをユーザ側に転送する。ユーザ側では、転送された音楽データを例えばパーソナルコンピュータのハードディスクに保存し、必要に応じて所定の再生手段によって再生する。

【0004】

【発明が解決しようとする課題】このような音楽配信システムでは、通常、ユーザが音楽配信サーバから音楽デ

ータをダウンロードする際に課金が発生する。すなわち、例えば1音楽データ、あるいは、1回のダウンロードにつき所定の金額を音楽配信サーバ側に支払うことで、ユーザはダウンロードを許可され、所望の音楽データを入手することができる。従来では、このようなシステムに関し、同一のユーザが過去に課金されダウンロードした音楽データを再度ダウンロードする際にも、再び課金となってしまうという問題点があった。

【0005】また、音楽データは、デジタルデータとして配信される。そして、配信された音楽データは、上述したように、ユーザによって、デジタルデータとして保存される。デジタルデータは、周知のように、劣化無く何度でも複製が可能である。そのため、従来では、ダウンロードされた音楽データの著作権を保護することが非常に難しいという問題点があった。

【0006】さらに、この問題に対処するために、音楽データを所定の暗号化方式で暗号化し、ユーザは、音楽配信サーバ側から予め与えられた鍵で、暗号化された音楽データを復号化する方法も考えられる。しかしながら、この方法でも、何らかの方法で暗号化された音楽データの鍵が破られてしまった場合、対処する方法が無いという問題点があった。

【0007】したがって、この発明の目的は、ユーザに対して2重に課金するようなことが無いような音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。

【0008】また、この発明の別の目的は、音楽データの著作権の保護に対して十分な配慮がなされた音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。

【0009】また、この発明のさらに別の目的は、音楽データのセキュリティに対して十分な配慮がなされた音楽配信方法、送信装置および方法、ならびに、再生装置および方法を提供することにある。

【0010】

【課題を解決するための手段】この発明は、上述した課題を解決するために、端末装置から要求された音楽データを、端末装置に対して配信する音楽配信方法において、端末装置からの音楽データ配信の要求を受け付ける第1のステップと、要求に基づき音楽データを端末装置に対して配信する第2のステップと、要求があった端末装置の識別情報と、要求された音楽データとを関連付ける管理情報を蓄積する第3のステップと、要求に基づき課金処理を行う第4のステップとを有し、第1のステップで端末装置から音楽データ配信の要求を受け付けたときに、第3のステップでの管理情報に基づき、端末装置による音楽データ配信に対して第4のステップでの課金処理による課金が過去に行われていると判断された場合、第4のステップで、課金をしないように処理するようにしたことを特徴とする音楽配信方法である。

【0011】また、この発明は、端末装置から要求された音楽データを、端末装置に対して配信する送信装置において、音楽データを保存する音楽データ保存手段と、端末装置からの音楽データ配信の要求を受信する受信手段と、受信手段によって受信された要求に基づき音楽データ保存手段から音楽データを出力する音楽データ出力手段と、音楽データ出力手段によって出力された音楽データに対して暗号化を施す暗号化手段と、暗号化された音楽データを端末に対して送信する送信手段とを有することを特徴とする送信装置である。

【0012】また、この発明は、記憶媒体に記憶されたデジタルオーディオデータからなる音楽データを再生する再生装置において、他の再生装置と区別するための識別情報を保持する識別情報保持手段と、暗号化された音楽データが記憶される音楽データ記憶手段と、音楽データ記憶手段に記憶されている音楽データを読み出し、暗号を復号化する復号化手段と、復号化手段から出力された音楽データをアナログ変換して音声信号として出力する音声信号出力手段とを有することを特徴とする再生装置である。

【0013】また、この発明は、端末装置から要求された音楽データを、端末装置に対して配信する送信方法において、音楽データを保存する音楽データ保存のステップと、端末装置からの音楽データ配信の要求を受信する受信のステップと、受信のステップによって受信された要求に基づき音楽データ保存のステップで保存された音楽データを出力する音楽データ出力のステップと、音楽データ出力のステップによって出力された音楽データに対して暗号化を施す暗号化のステップと、暗号化された音楽データを端末に対して送信する送信のステップとを有することを特徴とする送信方法である。

【0014】また、この発明は、記憶媒体に記憶されたデジタルオーディオデータからなる音楽データを再生する再生方法において、他の再生装置と区別するための識別情報を保持する識別情報保持のステップと、暗号化された音楽データが記憶される音楽データ記憶のステップと、音楽データ記憶のステップに記憶されている音楽データを読み出し、暗号を復号化する復号化のステップと、復号化のステップから出力された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする再生方法である。

【0015】また、この発明は、端末装置からサーバに対して音楽データの配信が要求され、要求に基づきサーバから端末装置に対して音楽データの配信を行う音楽配信方法において、端末装置からサーバに対して音楽データ配信を要求する音楽データ配信要求のステップと、音楽データ配信要求のステップで要求された音楽データが端末装置に対して過去に配信したことがあるかどうか調べられ、その結果に基づき、新規の要求であるとされれば課金を行い、過去に配信したことがあるとされれば

課金を行わない課金処理のステップと、音楽データ配信要求のステップで要求された音楽データに対して、予め作成された、端末装置に固有の第1の鍵で暗号化を施す暗号化のステップと、暗号化された音楽データを端末装置に送信する送信のステップと、送信のステップで送信された音楽データを受信し、記憶媒体に記憶する記憶のステップと、記憶媒体から音楽データを読み出し、読み出された音楽データに施されている暗号を、予め作成された端末装置に固有の第2の鍵で、読み出しに伴い復号化する復号化のステップと、復号化された音楽データをアナログ変換して音声信号として出力する音声信号出力のステップとを有することを特徴とする音楽配信方法である。

【0016】上述したように、請求項1に記載の音楽配信方法によれば、音楽データの配信要求があった端末装置と既になされた課金処理とが関連付けられた管理情報に基づき、今回配信が要求された音楽データに対して既に課金されていれば、今回は課金されないように課金処理がなされるため、同一の音楽データに対して重複して課金されることがない。

【0017】また、請求項2または9に記載の送信装置または方法によれば、配信を要求された音楽データを、暗号化を施して送信するため、送信された音楽データの著作権が保護される。

【0018】また、請求項5または10に記載の再生装置または方法によれば、他の再生装置と区別するための識別情報が保持されると共に、暗号化が施されたまま記憶媒体に記憶された音楽データを、記憶媒体から読み出しながら暗号の復号化を行い、復号化された音楽データをアナログ変換して音声信号として再生するため、記憶媒体に記憶されている音楽データの著作権が保護される。

【0019】また、請求項11に記載の音楽配信方法によれば、端末装置からサーバに対して音楽データの配信が要求され、要求された音楽データがその端末装置に対して既に配信したことがあれば課金が行われず、新規に要求されたものであれば課金が行われると共に、音楽データは、予め作成された、端末装置に固有の第1の鍵で暗号化されて端末装置に対して送信され、送信された音楽データを受信した端末装置では、受信された音楽データが記憶媒体に記憶され、再生時に記憶媒体から読み出された音楽データに対して、予め作成された、端末装置に固有の第2の鍵で暗号の復号化が行われるため、同一の音楽データの配信要求に対して重複して課金が行われないと共に、音楽データが端末装置に固有の鍵で暗号化/復号化されるため、音楽データの著作権が保護される。

【0020】

【発明の実施の形態】以下、この発明の実施の一形態を、図面を参照しながら説明する。図1は、この発明に適用できる音楽配信システムの構成の一例を示す。例え

ばインターネットであるネットワーク1に対して、音楽データの配信を受ける側であるクライアント2が多数、接続される。また、ネットワーク1に対して、音楽データの配信を行う側である音楽配信サーバ3が接続される。

【0021】この例では、ユーザすなわちクライアント2と音楽配信サーバ3との間で、特定の契約が交わされることによって、音楽配信サーバ3からクライアント2に対する音楽データの配信を行うことができるようになる。契約されたクライアント2から音楽配信サーバ3に対して、ネットワーク1を介して音楽データのダウンロードが要求される。音楽配信サーバ3は、この要求に基づき、音楽データを、ネットワーク1を介して要求のあったクライアント2に対して送信し、音楽データの配信を行う。

【0022】音楽データは、暗号化されて配信される。クライアント2では、配信された音楽データを暗号化されたまま保存する。暗号化の方式としては、例えば公開鍵方式を用いることができる。これは、周知のように、暗号化のための鍵である公開鍵と、暗号を解読するための鍵である秘密鍵との、2つの鍵を用いる方式である。2つの鍵は、暗号を送られる側で作成される。公開鍵は、暗号化を行う側に送られ、秘密鍵は暗号を送られる側で保存される。公開鍵で作成された暗号は、対応する秘密鍵でしか解読できない。

【0023】クライアント2は、この音楽配信システムの端末装置として構成され、例えばパーソナルコンピュータ10と、パーソナルコンピュータ10と所定のインターフェイスによって接続可能な携帯用オーディオ再生装置11とからなる。携帯用オーディオ再生装置11の代わりに、据置型オーディオ再生装置12を備えてもよい。これら再生装置11および12は、オーディオデータの記録の機能を有していてもよい。

【0024】音楽配信サーバ3は、複数のサーバからなるシステムである。音楽配信サーバ3は、暗号鍵サーバ20、認証システム21、音楽データベース22および課金システム23を有する。

【0025】暗号鍵サーバ20は、公開鍵の管理などを行うと共に、配信される音楽データの暗号化を行う。音楽データベース22には、デジタルオーディオデータからなる音楽データが多数、蓄積されており、ユーザからの音楽データの配信要求に基づき、音楽データの検索を行う。認証システム21は、ユーザに関する情報が管理されたユーザデータベースを有し、ユーザ情報が蓄積されると共に、音楽データの配信を要求してきたユーザが正規のユーザであるかどうかの認証を行う。また、課金システム23は、音楽データの配信を要求してきたユーザのうち、課金を行うべきユーザに対して課金処理を行う。これらのサーバならびにシステム間では、互いに情報の参照を行うことができる。

【0026】なお、音楽データベース22に蓄積されている音楽データは、所定の方式で圧縮符号化される。これは、圧縮符号化されて音楽データベース22に蓄積されるようにしてもよいし、音楽データベース22から出力されてから圧縮符号化するようにしてもよい。圧縮符号化の方式としては、ATRAC (Adaptive Transform Acoustic Coding: 商標)、ATRACが改良されたATRAC2 (商標)、MPEG (Moving Picture Experts Group) オーディオ、TwinVQ (商標) など、様々な方式を用いることができる。

【0027】クライアント2から音楽配信サーバ3に対して、ネットワーク1を介して音楽データの配信が要求される。このとき、予めユーザに与えられた認証用IDが音楽配信サーバ3に対して送信される。この認証用IDが認証システム21で確認され、正規のユーザからの要求であるとされると、音楽データベース22に対して要求された音楽データの検索が指示されると共に、課金システム23に対して、そのユーザに対する課金処理を行う指示が出される。検索された音楽データは、暗号鍵サーバ20で、予め認証サーバ21に登録されている、クライアント2の公開鍵で以て暗号化され、ネットワーク1を介して要求を出したクライアント2に対して送信される。

【0028】クライアント2では、音楽配信サーバ3から配信された音楽データは、暗号化されたまま、例えば一旦パーソナルコンピュータ10に保存され、音楽データのダウンロードがなされる。そして、音楽データは、暗号化されたまま携帯用オーディオ再生装置11に転送される。携帯用オーディオ再生装置11は、使用時にはパーソナルコンピュータ10と切り離して用いられ、パーソナルコンピュータ10から転送された音楽データの再生がなされる。音楽データは、携帯用オーディオ再生装置11において、上述の公開鍵と共に予め作成された秘密鍵で以て、暗号化を解かれながら再生される。

【0029】なお、課金は、例えば図示されない専用の回線により課金システム23クライアント2とが接続され、月毎などの単位で集計され、所定の金融機関から引き落とすようにされる。これに限らず、例えばプリペイドカードを利用しその都度支払うようにしてもよい。

【0030】また、図1の構成は、この例に限定されない。例えば、ネットワーク1の代わりに、衛星を利用した通信システムを用いることができる。この場合、クライアント2と音楽配信サーバ3とは、所定の回線、例えば公衆電話回線で接続される。この回線を通じて、クライアント2から音楽配信サーバ3に対して音楽データの配信要求が出される。音楽配信システム3では、この要求に基づき音楽データベース22が検索され、衛星を介してクライアント2に対して音楽データの配信が行われる。

【0031】図2は、携帯用オーディオ再生装置11の

構成の一例を示す。この例では、再生装置11は、音楽データの記録媒体として半導体メモリを用いた携帯用ヘッドフォンステレオ11である。F-ROM30は、音楽データを記憶するためのフラッシュメモリである。F-ROM30は、電氣的に内容の消去を行い、データを書き替えることができる。F-ROM30は、メモリコントローラ31によって、データの読み出しや書き替えの制御が行われる。例えば、外部インターフェイス39から供給された音楽データは、メモリコントローラ31の制御によってF-ROM30に書き込まれる。

【0032】なお、メモリコントローラ31は、後述するシスコン36の制御に基づき、F-ROM30から読み出された音楽データを、秘密鍵を用いて復号化する機能を有する。この復号化の処理は、音楽データの読み出しに伴い、リアルタイムで行われる。

【0033】メモリコントローラ31の制御によってF-ROM30から音楽データが読み出され、暗号の復号化がなされ、デコーダ32に供給される。音楽データは、所定の方式、例えばATRAC2方式で圧縮符号化されている。このデコーダ32で、この圧縮符号化が解かれデジタルオーディオデータとされた音楽データは、DSP33に供給される。

【0034】DSP33は、後述するシスコン36からのコマンドにより、供給されたデジタルオーディオデータに対して所定の処理、例えばイコライジング処理やレベル調整処理などを施す。DSP33から出力されたデジタルオーディオデータは、図示されないD/A変換器によってアナログオーディオ信号に変換され、アナログアンプ34に供給される。そして、所定のレベルまで増幅され、例えばヘッドフォン35に供給され、再生音声とされる。

【0035】外部インターフェイス39は、F-ROM30に対して音楽データの転送を行う際に用いられるインターフェイスである。外部インターフェイス39と後述するパーソナルコンピュータ10の対応するインターフェイスとが所定のケーブルで接続され、パーソナルコンピュータ10からこの携帯用ヘッドフォンステレオ11に対して音楽データなどの転送が行われる。なお、インターフェイスはこれに限らず、例えば赤外線信号を利用したワイヤレスのものをを用いることもできる。

【0036】シスコン36は、CPU、ROMおよびRAMなどを有し、この携帯用ヘッドフォンステレオ11の全体を制御する。ROMには、初期プログラムやこの携帯用ヘッドフォンステレオ11のシリアル番号などが予め記憶される。ROMには、書き替え可能なフラッシュROMを用いるようにできる。また、RAMは、CPUが動作するためのワークメモリである。シスコン36によって、上述したメモリコントローラ31、デコーダ32およびDSP33が制御される。

【0037】操作部37は、ユーザの操作に基づきシス

コン36に対して制御信号を供給する。また、表示部38は、例えば液晶ディスプレイ(LCD)であり、シスコン36から供給される表示信号に基づく表示を行う。

【0038】例えば、F-ROM30に書き込まれている音楽データの曲名リストが表示部38に表示される。ユーザは、この表示に基づき操作部37を操作し、所望の音楽データの再生を指示する。この指示に基づく制御信号がシスコン36に供給される。この制御信号によってシスコン36によってメモリコントローラ31が制御され、F-ROM30から該当する音楽データが読み出される。読み出された音楽データは、メモリコントローラ31、デコーダ32、DSP33およびアナログアンプ34でそれぞれ所定の処理をされ、ヘッドフォン35で再生される。

【0039】図3は、パーソナルコンピュータ10の構成の一例を示す。この例では、パーソナルコンピュータ10は、一般的な構成を有し、例えばバス50に対してCPU51、RAM52およびROM53が接続されると共に、図示されないディスプレイアダプタを介してディスプレイ54が接続される。RAM52は、CPU51のワークメモリであり、ROM53には、初期プログラムなどが予め記憶される。

【0040】また、バス50に対して、さらに、ハードディスクドライブ(HDD)55が接続されると共に、入出力インターフェイス56が接続される。入出力インターフェイス56は、このパーソナルコンピュータ10外部とのデータのやり取りを司る。入出力インターフェイス56には、例えばキーボード58やマウス59、フロッピーディスクやMO(Magneto-Optical disc)などの着脱自在な記録媒体を用いる外部記憶装置61、ネットワーク1や公衆電話回線などと通信を行うためのモデム58が接続される。

【0041】また、入出力インターフェイス56には、上述した携帯用ヘッドフォンステレオ11との通信を行うためのインターフェイス57が接続される。すなわち、このインターフェイス57と、上述の携帯用ヘッドフォンステレオ11の外部インターフェイス39とが所定のケーブルで接続される。これにより、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に対する音楽データの転送が行われる。

【0042】音楽配信サーバ3からネットワーク1を介して配信された音楽データは、モデム58で受信され、入出力インターフェイス56およびバス50を介してHDD55に一旦書き込まれる。音楽データは、HDD55から読み出され、バス50および入出力インターフェイス56とを介してインターフェイス57に供給される。そして、インターフェイス57から携帯用ヘッドフォンステレオ11の外部インターフェイス39に対して供給される。

【0043】次に、この実施の一形態による、音楽デー

タのダウンロードの方法について説明する。図4は、ダウンロードの際の処理を概略的に示すフローチャートである。図4では、携帯用ヘッドフォンステレオ11、パーソナルコンピュータ10からなるクライアント2、および、音楽配信サーバ3のそれぞれの処理が互いに関連されて示されている。なお、以下の図中では、携帯用ヘッドフォンステレオは、携帯用HSあるいは単にHSと省略されて示されている。

【0044】先ず、この図4に示される処理の開始に先んじて、携帯用ヘッドフォンステレオ11とパーソナルコンピュータ10とが所定のインターフェイスによって接続され、互いに通信可能な状態とされる。そして、携帯用ヘッドフォンステレオ11では、図4のステップS21の「N」で示されるように、パーソナルコンピュータ10との通信待ちの状態とされる。また、音楽配信サーバ3でも、パーソナルコンピュータ10との通信待ち状態とされる（ステップS25の「N」）。

【0045】ユーザは、音楽配信サーバ3に対する音楽データのダウンロードの要求を、パーソナルコンピュータ10に対して指示する。この指示が出されると、先ず、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に対して、認証用IDが要求される（ステップS10）。そして、パーソナルコンピュータ10は、携帯用ヘッドフォンステレオ11からの認証用IDの受信待ち状態とされる（ステップS11の「N」）。

【0046】パーソナルコンピュータ10からの要求は、インターフェイス57を介して携帯用ヘッドフォン11に対して送信される。携帯用ヘッドフォン11では、この要求が外部インターフェイス39およびメモリコントローラ31を介してシスコン36に供給される。そして、受け取ったこの要求に基づき、パーソナルコンピュータ10に対して認証用IDを送信する（ステップS22）。

【0047】認証用IDは、例えば、この携帯用ヘッドフォンステレオ11のそれぞれに対して予め与えられ、シスコン36のROMに記憶された、ユニークなシリアル番号を用いることができる。この認証用IDは、例えば、この携帯用ヘッドフォンステレオ11の出荷時などに、認証用サーバ21のユーザデータベースに対して予め登録しておくことができる。

【0048】この認証用IDがパーソナルコンピュータ10に受信されたら（ステップS11の「Y」）、処理はステップS12に移行し、パーソナルコンピュータ10から音楽配信サーバ3に対して、認証用IDに基づく認証の確認が要求される。そして、パーソナルコンピュータ10は、音楽配信サーバ3からの認証結果待ちとされる（ステップS13の「N」）。

【0049】音楽配信サーバ3では、パーソナルコンピュータ10からの認証の確認要求の送信を受けると（ステップS25の「Y」）、認証システム21においてユ

ーザデータベースが参照され、送られた認証用IDの確認が行われる。認証結果は、パーソナルコンピュータ10に送信される（ステップS26）。

【0050】認証結果が送信されると、音楽配信サーバ3側は、パーソナルコンピュータ10からの音楽データのダウンロード要求待ちとされる（ステップS27の「N」）。

【0051】音楽配信サーバ3からの認証結果がパーソナルコンピュータ10に受信されると（ステップS13の「Y」）、処理はステップS14に移行し、認証結果の判定が行われる。そして、認証の結果、認証要求を送信したパーソナルコンピュータ10が音楽データの配信を受けるのが不適切である（NG）と判断されると、処理はステップS15に移行し、ユーザに対して理由が通知され、一連の処理が終了される。音楽データの配信を受けるのが不適切である理由としては、例えば、（1）認証用IDが登録されているものではなく、そのユーザが正規ユーザではないと判断された場合、（2）複数の互いに異なるユーザから同一の認証用IDが送信された場合、などが挙げられる。パーソナルコンピュータ10のディスプレイ54上に、これらの情報が表示される。

【0052】なお、同一ユーザから互いに異なる複数の認証用IDが送られてきた場合には、その認証用IDでの使用を不可とすると良い。また、上述の（2）の例としては、ハードウェアをリバースエンジニアなどでまると不正コピーされた場合が考えられる。

【0053】一方、ステップS14で、認証の結果、認証要求を送信したパーソナルコンピュータ10が音楽データの配信を受けるのが適切である（OK）であると判断されると、処理はステップS16に移行し、パーソナルコンピュータ10から音楽配信サーバ3に対して、音楽データのダウンロード要求が出される。

【0054】例えば、音楽配信サーバ3が有する音楽データのリストに基づき、ユーザによって所望の音楽データが選択される。パーソナルコンピュータ10に対して選択された音楽データを表す情報が入力され、音楽配信サーバ3に対する音楽データのダウンロード要求が出される。

【0055】音楽データのリストは、音楽配信サーバ3側からユーザに対して配付される。ネットワーク1を介して、ユーザが音楽配信サーバ3から得られるようにしてもよい。これに限らず、パーソナルコンピュータ11からネットワーク1を介して音楽データベース22に対してアクセスし、所望の音楽データを検索するようにもできる。

【0056】音楽配信サーバ3側では、ステップS27にてパーソナルコンピュータ10からの音楽データのダウンロード要求が受信される。そして、次のステップS28で、音楽データベース22に対して、ダウンロードが要求された音楽データの検索が行われる。検索された

音楽データは、ステップS29で、そのユーザから送られた公開鍵で以て暗号化され、パーソナルコンピュータ10に送信される。このステップS29での処理については後述するが、このときに、ユーザに対する課金処理も行われる。

【0057】なお、図示しないが、音楽データが送信される際、その旨がユーザ情報と対応付けられて認証システム21のユーザデータベースに格納される。ユーザから音楽データのダウンロード要求があった場合に、このユーザデータベースが参照され、過去にそのユーザに対して該当音楽データをダウンロードしたかどうか、また、そのときの課金情報が調べられる。これにより、同一のユーザが同一の音楽データをダウンロードする際に重複して課金されるのを防ぐことができる。

【0058】パーソナルコンピュータ10では、ステップS17のダウンロード待機状態にて、音楽配信サーバ3から送信された音楽データが受信され、音楽データのダウンロードがなされる。次のステップS18でダウンロードされた音楽データの保存先が指定される。この例では、音楽データの保存先を、パーソナルコンピュータ10のハードディスク55と、携帯用ヘッドホンステレオ11とから選択して指定できる。パーソナルコンピュータ10のハードディスク55への保存を選択した場合は、処理はステップS19へ移行し、ダウンロードされた音楽データがハードディスク55に保存され、一連の処理が終了される。なお、音楽データは、暗号化されたまま、ハードディスク55に保存される。

【0059】一方、ステップS18で、音楽データの保存先を、携帯用ヘッドホンステレオ11に選択した場合、処理はステップS20に移行する。そして、ダウンロードされた音楽データが携帯用ヘッドホンステレオ11に転送される。

【0060】音楽データは、インターフェイス57を介して携帯用ヘッドホンステレオ11に転送される。携帯用ヘッドホンステレオ11側では、音楽データは、外部インターフェイス39から供給され（ステップS23）、メモリコントローラ31を介してF-ROM30に保存される（ステップS24）。この場合も、音楽データは、暗号化されたままF-ROM30に保存される。

【0061】次に、上述のステップS29での、音楽配信サーバ3における音楽データの暗号化ならびにパーソナルコンピュータ10への転送の処理について、図5のフローチャートを用いて説明する。ステップS291は、上述のサーバ3側の処理における、ステップS25～ステップS28の処理である。ステップS292で、ダウンロード要求された音楽データが同一ユーザによって既にダウンロードされたデータであるかが判断される。これは、上述したように、認証システム21が有するユーザデータベースを参照することで判断され

る。

【0062】若し、今回ダウンロードを要求された音楽データがそのユーザによって過去にダウンロードされたことがあるものであると判断されたら、処理はステップS294に移行する。

【0063】一方、ステップS292で、今回ダウンロード要求が出された音楽データが、そのユーザによって過去にダウンロードされている音楽データではないとされたら、処理はステップS293に移行し、課金システム23によって課金処理が行われる。この課金処理によって、そのユーザに対して、所定金額を支払うような指示が出される。

【0064】そして、ステップS294で、ダウンロード要求された音楽データに対して、予めそのユーザから送られ、認証システム21に登録されている公開鍵による暗号化が施される。暗号化された音楽データは、次のステップS295で、パーソナルコンピュータ10に対して転送される。

【0065】次に、認証システム21に対して、新規に認証用IDを登録する際の手順の例について、図6のフローチャートを用いて説明する。なお、このフローチャートが実行されるのに先立って、携帯用ヘッドホンステレオ11とパーソナルコンピュータ10とが所定のインターフェイスによって接続され、互いに通信可能な状態とされる。

【0066】まず、ステップS30で、パーソナルコンピュータ10から携帯用ヘッドホンステレオ11に対して認証用IDが要求される。携帯用ヘッドホンステレオ11では、パーソナルコンピュータ10との通信待ちの状態（ステップS36の「N」）において、この要求が受信されると（ステップS36の「Y」）、次のステップS37で、パーソナルコンピュータ10に対して認証用IDが送信される。

【0067】パーソナルコンピュータ10では、認証用ID受信待ちの状態（ステップS31の「N」）においてこの認証用IDを受信すると、次のステップS32で、受信された認証用IDに基づき、公開鍵と秘密鍵とが作成される。作成された公開鍵は、認証システム21に送信される（ステップS33）。また、公開鍵と共に、そのユーザの認証用IDや、ユーザID、パスワードなども送られる。

【0068】音楽配信サーバ3側では、パーソナルコンピュータ10からの鍵の受信待ちの状態（ステップS40の「N」）において、この公開鍵が受信されると（ステップS40の「Y」）、処理は次のステップS41に移行する。ステップS41では、認証システム21で、受信された認証用IDのチェック、パスワードやユーザIDのチェックなどが行われる。そして、認証システム21のユーザデータベースに、受信された公開鍵が登録される。パーソナルコンピュータ10に送信される音楽

データは、登録された公開鍵を用いて暗号化される。

【0069】一方、パーソナルコンピュータ10では、ステップS32で作成された秘密鍵が携帯用ヘッドフォンステレオ11に対して転送される(ステップS34)。携帯用ヘッドフォンステレオ11では、秘密鍵の受信待ちの状態(ステップS38の「N」)で、パーソナルコンピュータ10から送られた秘密鍵を受け取ると(ステップS38の「Y」)、次のステップS39で、受信された秘密鍵を保存する。秘密鍵は、例えばシスコ36が有する、バッテリバックアップされたRAMに保存される。シスコ36のROMに書き込むようにしてもよい。これに限らず、F-ROM30の所定領域に保存されるようにしてもよい。

【0070】次に、ダウンロードされた音楽データを、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に転送し、再生する手順について、図7のフローチャートを用いて説明する。なお、この手順に先んじて、パーソナルコンピュータ10に対して、ユーザが固有に有するユーザIDとパスワードとが予め入力され、例えばハードディスク55の所定領域に記憶されているものとする。また、携帯用ヘッドフォンステレオ11固有の認証用IDがパーソナルコンピュータ10に予め記憶されており、ユーザIDおよびパスワードと関連付けられる。

【0071】図7のフローチャートにおいて、最初のステップS50で、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に対して認証用IDが要求される。携帯用ヘッドフォンステレオ11では、パーソナルコンピュータ10との通信待ちの状態(ステップS56の「N」)において、この要求が受信されると(ステップS56の「Y」)、次のステップS57で、パーソナルコンピュータ10に対して認証用IDが送信される。

【0072】パーソナルコンピュータ10では、認証用ID受信待ちの状態(ステップS51の「N」)においてこの認証用IDを受信すると、次のステップS52で、受信された認証用IDがチェックされる。このとき、パーソナルコンピュータ10上で、そのユーザに対して決められたユーザIDおよびパスワードの入力が要求される。チェックは、例えば、入力されたユーザIDおよびパスワードの組み合わせが判定されると共に、これらユーザIDおよびパスワードと、携帯用ヘッドフォンステレオ11固有の認証用IDとが互に対応するかどうかを調べることでなされる。

【0073】若し、これら認証用IDとユーザIDおよびパスワードとが所定の関係になければ、チェックの結果がNG(No Good)とされ、処理はステップS55に移行する。そして、ステップS55で、その理由がパーソナルコンピュータ10のディスプレイ上に表示される。一例としては、「ユーザIDあるいはパスワードが間違

っています」、「不正な認証用IDです」などと表示される。

【0074】一方、ステップS52で、認証用IDとユーザIDおよびパスワードとが所定の関係にあり、認証結果がOKであるとされれば、処理はステップS53に移行する。そして、ユーザにより選曲がなされ、パーソナルコンピュータ10から携帯用ヘッドフォンステレオ11に対して転送する音楽データが選択される。ステップS54で、選択された音楽データがヘッドフォンステレオ11に対して転送される。上述したように、音楽データは、ハードディスク55上に暗号化されたまま保存されている。ステップS54での転送も、音楽データが暗号化されたまま、行われる。

【0075】携帯用ヘッドフォンステレオ11側では、パーソナルコンピュータ10からの音楽データの転送待ちの状態(ステップS58の「N」)において、この音楽データが受信されると(ステップS58の「Y」)、次のステップS59で、受信された音楽データがF-ROM30に対して保存される。

【0076】携帯用ヘッドフォンステレオ11において、F-ROM30に保存された音楽データの再生がステップS60で指示される。この指示により、F-ROM30に保存された音楽データがメモリコントローラ31の制御に基づき読み出される。読み出された音楽データは、上述の図6のステップS39で、予め携帯用ヘッドフォンステレオ11に対して記憶された秘密鍵を用いて復号化されながら(ステップS61)、デコーダ32に供給される。

【0077】なお、秘密鍵による音楽データの復号化は、この例では、ハードウェア的に処理される。例えば、暗号を解くためのアルゴリズムが内蔵された集積回路に対して、秘密鍵がパラメータとして与えられ、暗号化された音楽データの復号化がなされる。また、これに限らず、ハードウェアが十分な処理速度を有していれば、ソフトウェア的な処理で復号化を行ってもよい。

【0078】音楽データは、デコーダ32で、音楽配信サーバ3側で施された圧縮符号化が解かれ(ステップS62)、DSP33に供給され所定の信号処理を施される。DSP33の出力は、図示しないD/A変換器によってアナログオーディオ信号に変換され(ステップS63)、アンプ34で増幅されヘッドホン35で再生される。

【0079】次に、この発明による、音楽データに対するセキュリティ、すなわち、著作権を保護するための機構について、図8を用いて説明する。クライアント2側では、携帯用ヘッドフォンステレオ11における、例えばユニークなシリアル番号を認知用IDとして、この認知用IDに基づいて秘密鍵101および公開鍵100を作成する。秘密鍵101は、携帯用ヘッドフォンステレオ11に保存され、公開鍵100は、サーバ3に送ら

れ、保存ならびに管理される。

【0080】既に述べたように、音楽データは、サーバ3からクライアント2に対して転送される際に、転送するユーザから送られた公開鍵によって暗号化される。また、携帯用ヘッドフォンステレオ11では、音楽データは、暗号化されたまま保存され、再生時に秘密鍵を用いて再生される。

【0081】そのため、クライアント2側では、こうして転送された音楽データは、公開鍵100と対応する秘密鍵101を有する携帯用ヘッドフォンステレオ11でしか再生できない。例えば、転送された音楽データをハードディスク55に保存し、別の携帯用ヘッドフォンステレオ11'（図示しない）で再生しようとしても、その携帯用ヘッドフォンステレオ11'は、公開鍵100に対応する秘密鍵101を有していないので、再生できない。したがって、音楽データを複製しても、複製された音楽データは、公開鍵100に対応する秘密鍵101を持たない他の機器では再生できず、その音楽データの著作権が保護されることになる。

【0082】また、何らかの方法で秘密鍵101が破られてしまった場合でも、対応が可能である。一例として、例えば悪意の第三者による秘密鍵の盗用などが行われた場合、その秘密鍵と対応する公開鍵をサーバ3側で消去すると共に、正規のユーザに対して、新しい認知用IDを配付する。これは、例えば携帯用ヘッドフォンステレオ11のファームウェアの書き替えを行い、シリアル番号を変更することでなされる。この新しい認知用IDに基づき、新規に、公開鍵100および秘密鍵101とを作成することで、盗用された秘密鍵を使用することができなくなる。

【0083】なお、上述では、音楽データの暗号化に公開鍵方式を用いているが、これはこの例に限定されない。例えばDES(Data Encryption Standard)方式といった、共通鍵方式を用いて音楽データの暗号化を行うようにしてもよい。この場合、共通鍵は、サーバ3からクライアント2へ、予め配付される。

【0084】また、上述では、音楽データは、携帯用ヘッドフォンステレオ11において再生時に復号化されるとしたが、これはこの例に限定されない。例えば、暗号化されたままF-ROM30に記憶された音楽データを、例えばバッファメモリなどを利用して予め復号化しておき、再びF-ROM30に書き戻すことも考えられる。

【0085】さらに、上述では、クライアント2においてパーソナルコンピュータ10を用いて端末装置が構成されているが、これはこの例に限定されない。他の情報機器、例えば衛星放送などを受信するためのセットトップボックスを、このパーソナルコンピュータ10の代わりに用いることもできる。また、この音楽配信に専用の情報機器を設けることもできる。

【0086】

【発明の効果】以上説明したように、この発明によれば、一度ダウンロードして課金された音楽データに対して、次のダウンロードからは課金がなされない。そのため、ユーザは、連続再生するだけの容量を有したハードディスクなどの記録媒体を用意すればよいという効果がある。

【0087】また、同じ音楽データに対して課金がなされないため、ユーザは、必要なときに音楽データのダウンロードを行うことができる。そのため、音楽データのバックアップなどを行う必要がないという効果がある。

【0088】さらに、この発明では、音楽データは、暗号化されてダウンロードされると共に、暗号化されたままユーザの下に保存される。そして、音楽データの再生は、再生装置に固有の鍵で復号化されながら行われる。そのため、音楽データの著作権が十分保証されるという効果がある。

【0089】さらにまた、この実施の一形態では、暗号化鍵が破られた場合にも対処可能であるという効果がある。

【図面の簡単な説明】

【図1】この発明に適用できる音楽配信システムの構成の一例を示す略線図である。

【図2】携帯用ヘッドフォンステレオの構成の一例を示すブロック図である。

【図3】パーソナルコンピュータの構成の一例を示すブロック図である。

【図4】音楽データのダウンロードの際の処理を概略的に示すフローチャートである。

【図5】音楽データの暗号化ならびにパーソナルコンピュータへの転送の処理を説明するためのフローチャートである。

【図6】認証システムに対して新規に認証用IDを登録する際の手順の一例を説明するためのフローチャートである。

【図7】ダウンロードされた音楽データをパーソナルコンピュータから携帯用ヘッドフォンステレオに転送し再生する手順を説明するためのフローチャートである。

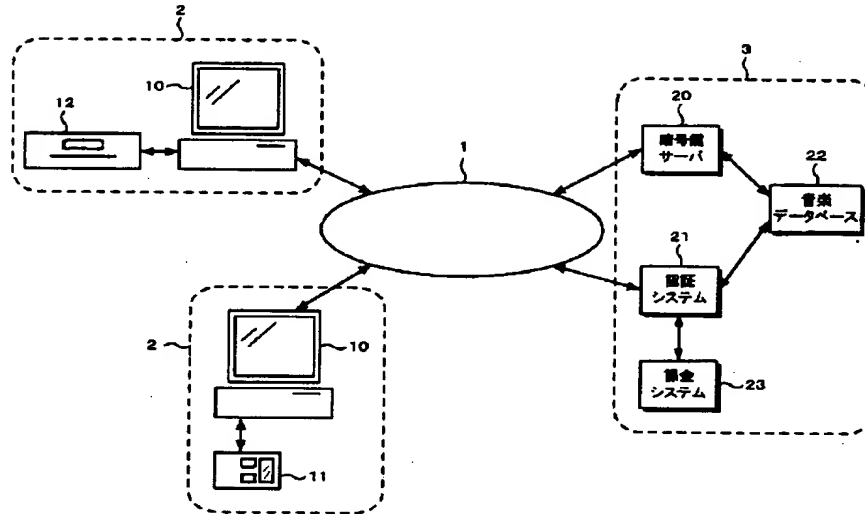
【図8】音楽データの著作権を保護するための機構について説明するための図である。

【符号の説明】

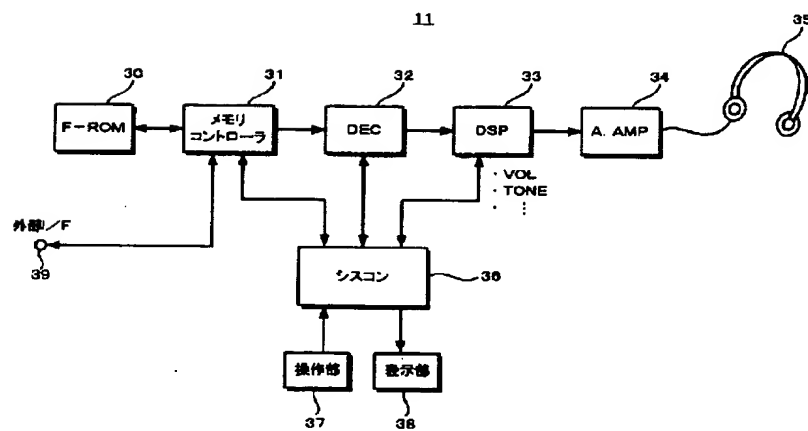
1・・・ネットワーク、2・・・クライアント、3・・・音楽配信サーバ、10・・・パーソナルコンピュータ、11・・・携帯用ヘッドフォンステレオ、20・・・暗号鍵サーバ、21・・・認証システム、22・・・音楽データベース、23・・・課金システム、30・・・フラッシュメモリ、31・・・メモリコントローラ、36・・・シスコン、39・・・外部インターフェイス、51・・・CPU、55・・・ハードディスク、57・・・携帯用ヘッドフォンステレオと接続するための

インターフェイス、100・・・公開鍵、101・・・ 秘密鍵

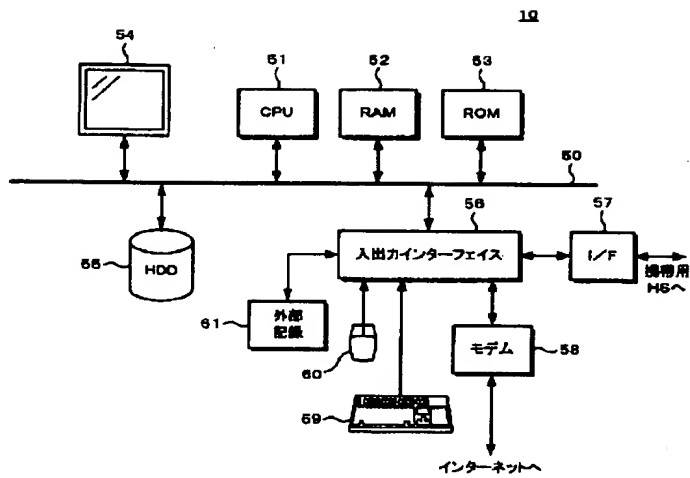
【図1】



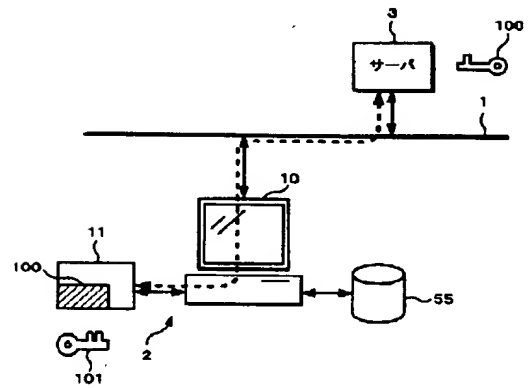
【図2】



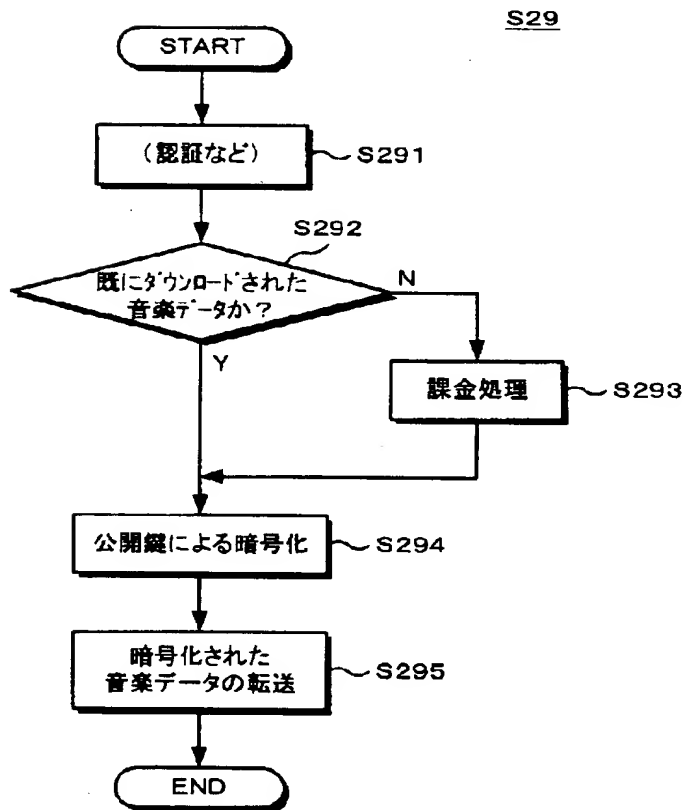
【図3】



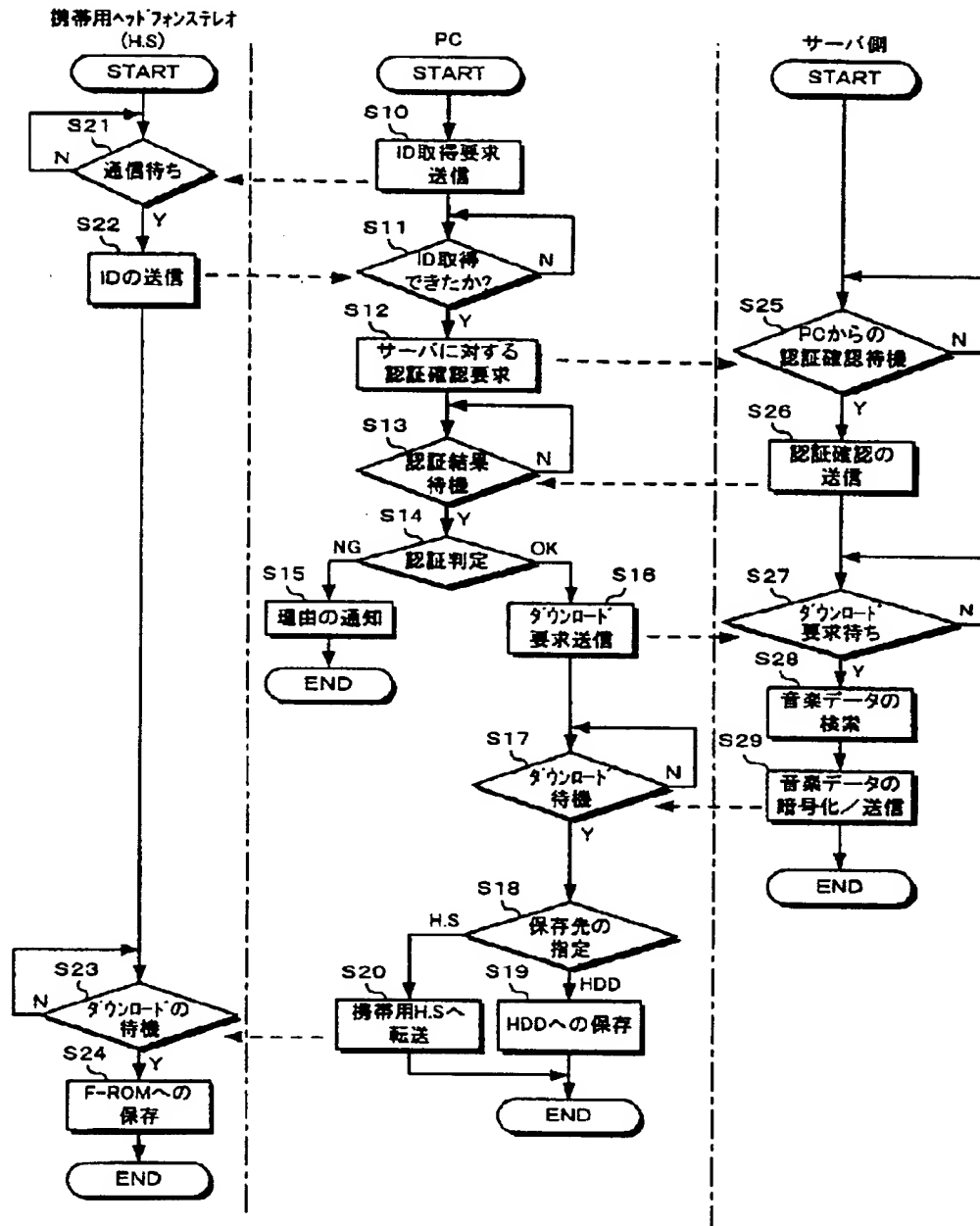
【図8】



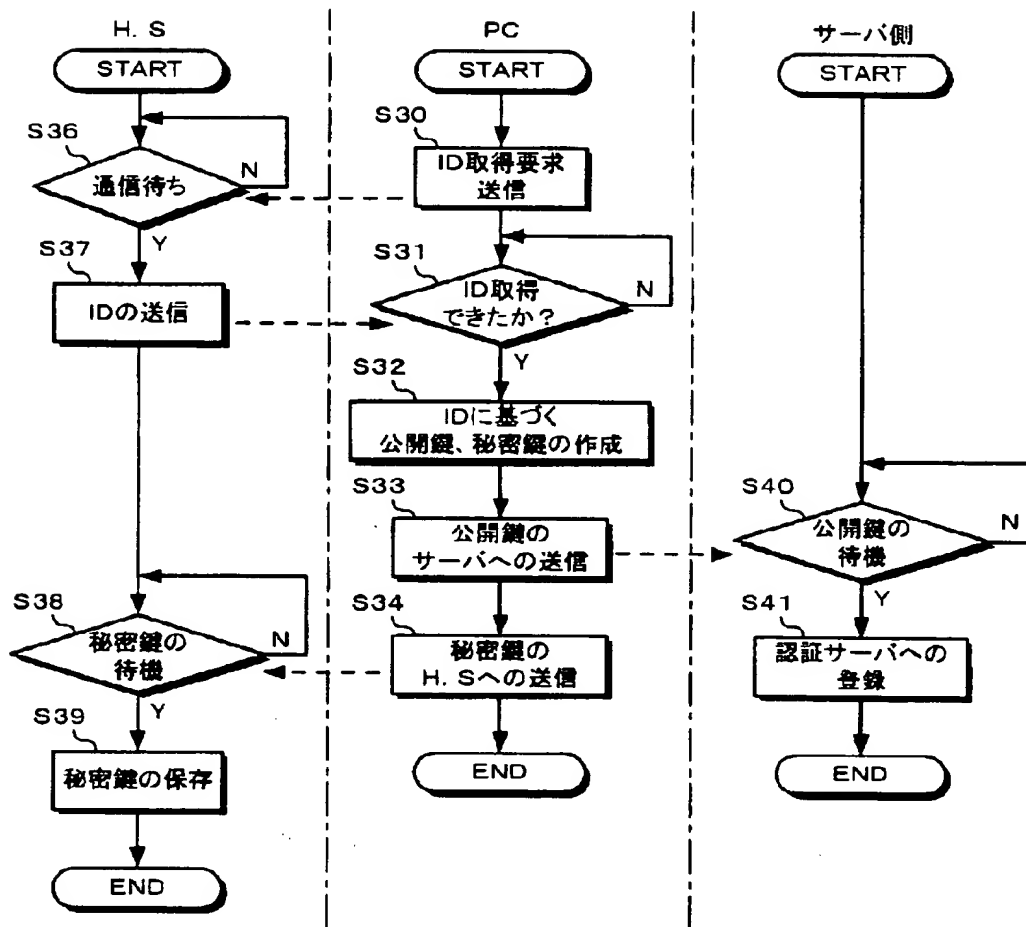
【図5】



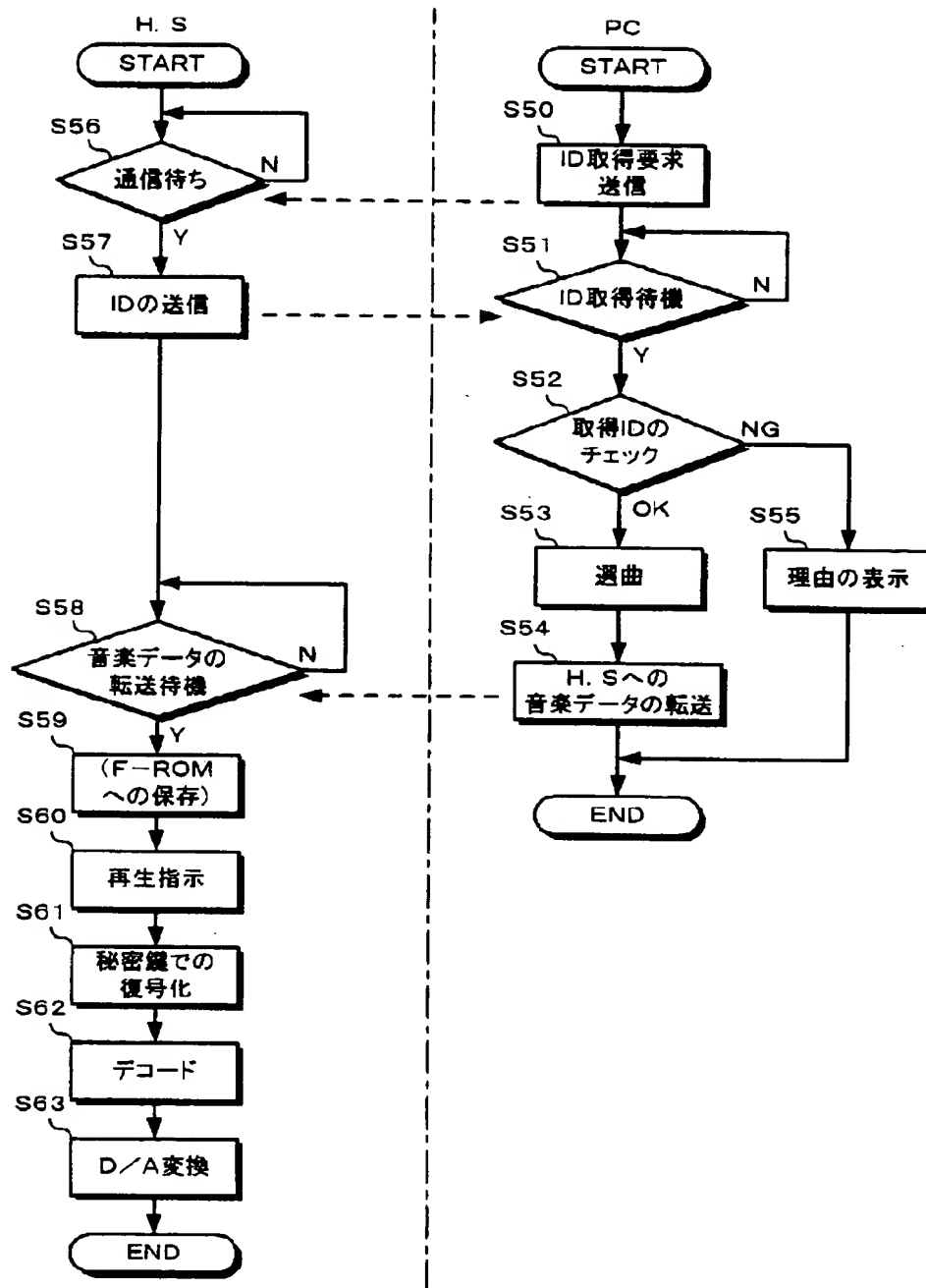
【図4】



【図6】



【図7】



フロントページの続き

Fターム(参考) 5B089 AA16 AA22 AB01 AC03 AD06
AE09 CE08 DD03 DD06 DD07
5D108 BA04 BA06 BC01 BF11 BF12
BF13 BF20 BH10
5K101 KK18 MM07 NN03 NN18 NN21
NN48 TT06 UU16 UU19 UU20
VV06